IN THE UNITED STATES COURT OF FEDERAL CLAIMS

3 RD EYE SURVEILLANCE, LLC	§
and DISCOVERY PATENTS, LLC	§
	§
Plaintiffs,	§
	§
V.	§ CIVIL ACTION NO. 15-501 C
	§
	§
THE UNITED STATES,	§
	§
Defendant.	§

FIRST AMENDED COMPLAINT

Plaintiffs 3rd Eye Surveillance, LLC ("3rd Eye") and Discovery Patents, LLC ("Discovery Patents") (together "Plaintiffs") files this First Amended Complaint against the United States of America and allege as follows:

PARTIES

- 1. Plaintiff 3rd Eye is a limited liability company organized under the laws of the State of Texas, with its principal place of business at 2616 Boedeker Drive, Plano, Texas 75074.
- Plaintiff Discovery Patents is a limited liability company organized under the laws
 of the State of Delaware with its principal place of business at 2015 Pig Neck Road, Cambridge,
 Maryland 21613.
- 3. The Defendant is the United States of America, acting through its various agencies, including by way of example, and not limitation, the Department of Justice, the Department of Homeland Security, USSTRATCOM, the Department of Defense, the United States Customs and Border Protection, the United States Army, the United States Navy, and the Defense Logistics Agency.

JURISDICTION

4. This is an action for patent infringement under 28 U.S.C. § 1498.

NATURE OF THE ACTION

- 5. This is an action for patent infringement against the United States to recover reasonable and entire compensation for the unlicensed use and manufacture by and for the United States of inventions claimed in:
 - a. U.S. Patent No. 6,778,085 (the "'085 Patent") titled "Security System and Method with Realtime Imagery," duly and lawfully issued on August 17, 2004, attached as Exhibit A;
 - b. U.S. Patent No. 6,798,344 (the "344 Patent") titled "Security Alarm System and Method with Realtime Streaming Video," duly and lawfully issued on September 28, 2004, attached as Exhibit B; and
 - c. U.S. Patent No. 7,323,980 (the "980 Patent") titled "Security System and Method with Realtime Imagery" duly and lawfully issued January 29, 2008, attached as Exhibit C. The patents are referenced herein together as the "Infringed Patents."
 - 6. 3rd Eye is the exclusive licensee of all rights to the Infringed Patents.
 - 7. Discovery Patents is the assignee of the Infringed Patents.
- 8. Otis Faulkner is a member of Discovery Patents and a co-inventor for each of the Infringed Patents.
- 9. The Government operates a series of security systems in airports, office buildings, and other locations that the Government considers locations that require monitoring.
- 10. Detailed specifications for the various Government security systems are confidential.

- 11. The Government enters into contracts with third parties for hardware components (such as cameras, audio sensors and computers/servers), software applications, and IT technology consulting necessary to implement and operate the infringing Government security systems.
- 12. The Government operates security systems at numerous secured locations, including, by way of example, and not limitation, airports, Federal Courts, and other government office buildings.

FACTS CONCERNING INFRINGING SYSTEM USED AT AIRPORTS

- 13. The Federal Government considers United States airports as secure locations.
- 14. The Federal Government has, on occasion, posted armed military personnel within airports, such as the Dallas Fort Worth International Airport, because it considers airports to be secure locations.
- 15. The Federal Government has installed security monitoring systems at airports because it considers airports to be secure locations.
- 16. Details concerning the security system or systems used at airports are confidential and secret.
- 17. The Government uses video cameras at airports to conduct surveillance. Figures 1 and 2 are photographs of separate video cameras used at different locations at DFW International airport:

Figure 1:

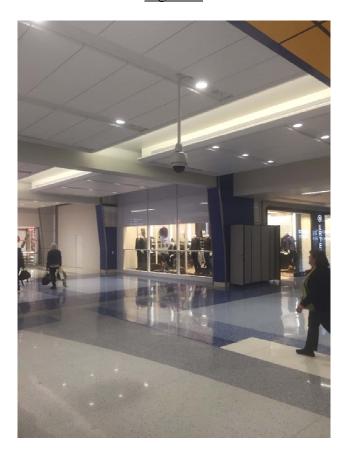


Figure 2



- 18. A January 12, 2016 news article appearing in the publication *Government Security*News describes an airport security monitoring system used by the Government. (Exhibit D)
- 19. The author of the article is an employee of a Government contractor, Hitachi Data Systems Federal ("Hitachi Federal"), which provides technology services to the Government.
- 20. In the article, the author indicates that the Government is using "video intelligence" and a "video intelligence platform" to provide an "automated" monitoring system.
- 21. The system in use includes cameras, sensors, a central collection station for receiving real time data by way of high speed internet or wireless technology, the employment of various communication links, and means to organize the data to alert an appropriate response agency such that data can be shared on a real time basis.
- 22. The system in use is described to specifically include video cameras and a wide range of disparate sensor data combined into a single portal.
- 23. The system in use is further described as one that is being used by the government and which permits law enforcement officials to analyze the data received from multiple sensors including video cameras, alarm systems, and GPS systems and organizes the data in such a way that patterns can be quickly detected.
 - 24. The system in use is further described as a data triage system.
- 25. The system in use is further described as one that can automate the monitoring process through the use of an intelligent video and sensor portal and operates on a scale that manpower cannot handle.
- 26. The system in use is further described as a video intelligence system that observes the behaviors of people and flags behaviors that indicate a higher security risk and subsequently provides that data to law enforcement for the purpose of making critical decisions.

- 27. The system in use includes an automated data collection system. The automated data collection allows for the integration of new behavioral models that are believed to exhibit dangerous activity. When the new behavioral models are integrated into the video intelligence system, the existing sensors identify additional examples of threatening behavior. The system is described to be flexible so that it may adapt to the changing tactics implemented by criminals at airports.
- 28. The system is further described as one that automates data collection, organization, and storage for the purpose of giving law enforcement the opportunity to prevent or respond to a terrorist attack with an effective security strategy.
 - 29. The system is further described as one that unifies data management.
- 30. The system is further described as one that can, among other things, distinguish between screaming in an airport-personnel corridor from loud music being played by a high school band in a public area of the airport.
- 31. The system is described to have the means to identify the correct government agency matching the specific threatening behavior that is being monitored through the video intelligence system.
- 32. The system is further described to include real time data, including video, for the purpose of establishing a common operating picture.
- 33. The system is further described as having a single portal, or central station, to analyze, view and store information.
- 34. The purpose of the central station for the collection of the data is to allow for the data to be shared with ease among various coordinating law enforcement agencies.

- 35. The system is further described as one that includes an interface for integration with an existing IT system, including a legacy IT system.
- 36. The system is further described as a video intelligence system that includes sensors, compute power, and on-board storage that can be installed and implemented rapidly.
- 37. The system is described as one that is implemented for use by Government personnel.
- 38. The "video intelligence system" is further described in a hyperlink that leads to the Hitachi Federal webpage. (Exhibit E) The "video intelligence system" is described by Hitachi Federal in Exhibit E as one that provides "end-to-end situational awareness and surveillance in a web-based, secure manager available for public, private and hybrid clouds." Hitachi Federal states that its system is "used by leading government agencies around the world and integrates with all major law enforcement systems." Hitachi Federal provides a link for an article entitled "Solutions for Public Safety and Smart Communities," which may be downloaded. (Exhibit F).
- 39. In the article, Hitachi Federal provides information regarding the Hitachi Visualization Platform (a turnkey hardware platform optimized for video-management-system processing and storage) and Hitachi Visualization Suite (a software application).
- 40. The Hitachi Visualization Suite provides "a common operating picture for full situational awareness." "It supports incident and investigative features, and connects with a wide range of security assets combined with powerful workflow and analytic capabilities." "It also includes a mobile application." "HVS analytic modules work as a data-mining engine to gather and even predict where and when crime can occur: They ingest real-time feed from open source, crime databases and online social media applications."

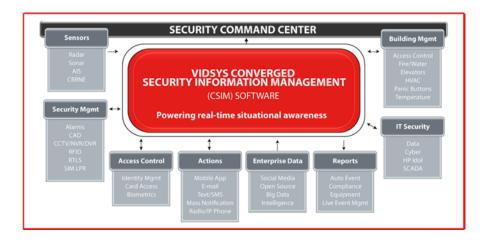
- 41. The Hitachi Visualization Suite modules "integrate 3rd-party video management software with critical sensors and systems to provide access control, video analytics, CAD and 911, GPS and mapping."
- 42. The Hitachi Federal software is proprietary and the source code comprising the software is not available to the public or Plaintiffs.
- 43. Plaintiffs do not allege that Hitachi Federal is directly or indirectly infringing the patents at this time.
- 44. The airport monitoring system in use by the Government infringes one or more of the '085 Patent claims, including, by way of example, and not limitation, Claim 1, because the airport monitoring system includes a security system comprising:
 - a. an imaging device positioned at a secured location, such as, by way of example, and not limitation, the video cameras seen above in Figures 1 and 2;
 - b. means, associated with a security system central station, for receiving and processing realtime imagery generated by said imaging device and received over a communications link, such as, by way of example, and not limitation, the system described in Exhibits D, E and F; and
 - c. means, associated with an emergency response agency, for receiving, processing and displaying realtime imagery generated by said imaging device and received over a communications link from the central station such as, by way of example, and not limitation, the system described in Exhibits D, E and F.
- 45. The airport monitoring system in use by the Government infringes one or more of the '344 Patent claims, including, by way of example, and not limitation, Claim 1, because the airport monitoring system includes a security alarm system comprising:

- a. a video camera such as, by way of example, and not limitation, the video cameras seen above in Figures 1 and 2;
- b. an alarm sensor positioned at a secured location such as, by way of example, and not limitation, the audio sensors described in Exhibits D, E and F;
- c. means, located a security system central station, for receiving, processing, and displaying realtime video generated by said video camera and received over a communications link such as, by way of example, and not limitation, the system described in Exhibits D, E and F;
- d. means for transmitting the realtime video from the central station to an emergency response agency over a communication link such as, by way of example, and not limitation, the system described in Exhibits D, E and F; and
- e. Means, located at the emergency response agency, for receiving processing and displaying realtime video by said video camera such as, by way of example, and not limitation, the system described in Exhibits D, E and F.
- 46. The airport monitoring system in use by the Government infringes one or more of the '980 Patent claims, including, by way of example, and not limitation, Claim 1, because the airport monitoring system includes a security system comprising:
 - a. An imaging device positioned at a secured location such as, by way of example, and not limitation, the cameras seen above in Figures 1 and 2;
 - A computer system associated with a security system central monitoring station,
 said computer system configured to:
 - i. receive real-time imagery data from said secured location;
 - ii. process the received imagery data;

- iii. generate additional information associated with the received imagery data;
- iv. identify an appropriate response agency from amongst a plurality of response agencies based on at least one of the additional information and the imagery data; and
- v. transmit the received imagery data and the additional information to a computer system associated with a response agency.
- 47. The airport monitoring system described and in use by the Government infringes one or more of the '980 Patent claims, including, by way of example, and not limitation, Claim 6, because the airport monitoring system includes a security system of Claim 1, wherein the additional information is voice data.
- 48. The airport monitoring system described and in use by the Government infringes one or more of the '980 Patent claims, including, by way of example, and not limitation, Claim 31, because the airport monitoring system includes a method of securing a location comprising the steps of:
 - a. generating real-time imagery of a secured location;
 - b. transmitting the real-time imagery to a security system central monitoring station over a network connection;
 - c. processing the real-time imagery at the security system central station;
 - d. transmitting the real-time imagery from the security system central station to a response agency over a network connection; and
 - e. displaying the real-time imagery at the response agency, wherein the response agency is identified from amongst a plurality of response agencies by a computer system at the security system central station.

FACTS CONCERNING INFRINGING SYSTEM USED FOR FEDERAL BUILDINGS

- 49. The Federal Government considers many federal buildings as secure locations.
- 50. One Government contractor, Vidsys, reported on its webpage that Federal Government buildings are dynamic environments that are often considered high threat targets and that Government facilities are attractive targets for terrorists and are a key component of the Department of Homeland Security Critical Infrastructure Protection Plan. (See Exhibit G)
- 51. Details concerning the security systems used at Government Buildings are confidential and secret.
- 52. Vidsys reports that it has one US federal client that has multiple buildings dispersed throughout the United States. Vidsys reports that it provides to this federal client Converged Security Information Management software (hereafter, "CSIM") and that CSIM is being used by the Government for application-specific tasks.
- 53. Vidsys indicates on its webpage that GSA Schedule 70 is the Federal Contract Vehicle through which it provides its services.
- 54. The CSIM software is proprietary and the source code comprising the software is not available to the public or Plaintiffs.
 - 55. Vidsys displays the following graphic to describe the services it is providing:



- 56. Vidsys provides a link to download a document it calls "The Government Solution Sheet." The document is attached hereto as Exhibit H.
- 57. Based on information made available by Vidsys, Plaintiffs allege that the Government is using the Vidsys CSIM software in connection with other components.
- 58. The Government's use of CSIM with other components as reported by Vidsys is infringing Plaintiffs' patents.
 - 59. The system described couples CSIM with sensors, including video cameras.
 - 60. The system described controls multiple and disparate systems and sensors.
 - 61. The system described prevents access to unauthorized areas.
 - 62. The system described includes real-time visibility of malicious threats.
 - 63. The system is described as effectively monitoring geographically dispersed assets.
- 64. The system described couples CSIM with sensors identified as video, radar, sonar, AIS and CBRNE.
- 65. The system described couples CSIM with security management such as alarms, CAD, CCTV/NVR/DVR, RFID, RTLS and SIM LPR.
- 66. The system described couples CSIM with access control including identity management, card access, and biometrics.
- 67. The system described couples CSIM with the capability of providing real-time data to emergency response agencies through a mobile app, email, text/sms, mass notification, and radio/IP phone.
- 68. The system described couples CSIM with enterprise data including social media data sources, open source data, so-called Big Data, and intelligence data.
 - 69. The system described provides reports for auto event and live event management.

- 70. The system described couples CSIM with open architecture computer systems and servers.
- 71. The system described is said to be capable of being integrated into virtually any computer system.
- 72. The system described couples CSIM with rapidly deployable browser-based content.
- 73. The system described includes a rules engine and work flow tool to give the federal government the ability to pre-determine what data should be correlated and what should be filtered out. By way of example, Vidsys reports that the system being used by the government includes a video analytics alert enabling a command center operator to be instantly presented with the exact location of the potential security breach and surrounding assets on a map, along with step-by-step instructions for evaluation and resolution, including pushing crucial information such as video camera views through the Vidsys mobile interface to a responding officer.
 - 74. The system described includes a central monitoring station.
 - 75. The system described includes the use of internet and wireless technology.
 - 76. The system described includes the use of computers and servers.
 - 77. The system described includes the use of sensors.
 - 78. The system described includes the identification of an appropriate response agency.
 - 79. Plaintiffs do not accuse Vidsys of patent infringement at this time.
- 80. Plaintiffs do not contend at this time that the Vidsys CSIM software, by itself, directly or indirectly, infringes the claims of Plaintiffs' patents.

- 81. The system in use by the Government infringes one or more of the '344 Patent claims, including, by way of example, and not limitation, Claim 1, because the system includes a security alarm system comprising:
 - a. a video camera and an alarm sensor positioned at a secured location;
 - means, located a security system central station, for receiving, processing, and displaying real-time video generated by said video camera and received over a communications link;
 - c. means for transmitting the real-time video from the central station to an emergency response agency over a communication link; and
 - d. Means, located at the emergency response agency, for receiving processing and displaying real-time video by said video camera.
- 82. The system described and in use by the Government infringes one or more of the '980 Patent claims, including, by way of example, and not limitation, Claim 1, because the system includes a security system comprising:
 - a. An imaging device positioned at a secured location;
 - A computer system associated with a security system central monitoring station,
 said computer system configured to:
 - i. receive real-time imagery data from said secured location;
 - ii. process the received imagery data;
 - iii. generate additional information associated with the received imagery data;
 - iv. identify an appropriate response agency from amongst a plurality of response agencies based on at least one of the additional information and the imagery data; and

- v. transmit the received imagery data and the additional information to a computer system associated with a response agency.
- 83. The system described and in use by the Government infringes one or more of the '980 Patent claims, including, by way of example, and not limitation, Claim 31, because the system includes a method of securing a location comprising the steps of:
 - a. generating real-time imagery of a secured location;
 - b. transmitting the real-time imagery to a security system central monitoring station over a network connection;
 - c. processing the real-time imagery at the security system central station;
 - d. transmitting the real-time imagery from the security system central station to a response agency over a network connection; and
 - e. displaying the real-time imagery at the response agency, wherein the response agency is identified from amongst a plurality of response agencies by a computer system at the security system central station.

FACTS CONCERNING INFRINGING SYSTEM USED FOR CUSTOMS AND BORDER PROTECTION

- 84. The Government protects its borders with fences, barricades and armed personnel.
- 85. Armed personnel, however, cannot monitor and secure the entire border.
- 86. The Government uses what it calls a "remote video surveillance system" or RVSS for the purpose of monitoring portions of its border.
- 87. The Government recently awarded a contract with a potential value of \$103 Million over ten years to General Dynamics One Source, a corporate entity comprised of General Dynamics Information Technology and General Dynamics Mission Systems for the purpose of upgrading its RVSS for border protection.

- 88. In an article dated October 14, 2015, appearing in Homeland Security Today, Mark Borkowski, the assistant commissioner and chief acquisition executive of CBP's Office of Technology and Acquisition, describes the functionality of the current RVSS and the capabilities of the upgraded system. See Exhibit I.
- 89. Borkowski states that "The [RVSS] is a critical element of our overall plan to secure the border...."
- 90. Located on elevated fixed towers and building structures, the RVSS includes a wide-area electro-optical and infrared multi-sensor camera system that provides Border Patrol agents with persistent ground surveillance and real-time video analytics to effectively detect, track, identify, classify, and respond to missions along the nation's borders.
- 91. As of October 14, 2015, General Dynamics had deployed a new command-and-control system and installed upgraded RVSS camera suites on five new and 12 legacy tower sites.
- 92. The RVSS upgrade increases the Border Patrol's situational awareness and improves efficiency and officer safety.
- 93. During a March 2011 hearing of the House Committee on Homeland Security Subcommittee on Border and Maritime Security, Borkowski stated in joint testimony with Border Patrol Chief Michael Fisher that "The new border security technology plan will utilize existing, proven technology tailored to the distinct terrain and population density of each border region, including commercially available Mobile Surveillance Systems, Unmanned Aircraft Systems [drones] thermal imaging devices and tower-based [RVSS]."
 - 94. The system includes the use of video cameras and infrared devices.
 - 95. The system uses computers and servers.

- 96. Images from the video and infrared sensors are transmitted to a central monitoring station.
 - 97. The system includes the use of internet and wireless technology.
 - 98. The system includes the use of computers and servers.
 - 99. The system includes the identification of an appropriate response agency.
- 100. The system in use by the Government infringes one or more of the '344 Patent claims, including, by way of example, and not limitation, Claim 1, because the system includes a security alarm system comprising:
 - a. a video camera and an alarm sensor positioned at a secured location;
 - means, located a security system central station, for receiving, processing, and displaying real-time video generated by said video camera and received over a communications link;
 - c. means for transmitting the real-time video from the central station to an emergency response agency over a communication link; and
 - d. Means, located at the emergency response agency, for receiving processing and displaying real-time video by said video camera.
- 101. The system described and in use by the Government infringes one or more of the '980 Patent claims, including, by way of example, and not limitation, Claim 1, because the system includes a security system comprising:
 - a. An imaging device positioned at a secured location;
 - A computer system associated with a security system central monitoring station,
 said computer system configured to:
 - i. receive real-time imagery data from said secured location;

- ii. process the received imagery data;
- iii. generate additional information associated with the received imagery data;
- iv. identify an appropriate response agency from amongst a plurality of response agencies based on at least one of the additional information and the imagery data; and
- v. transmit the received imagery data and the additional information to a computer system associated with a response agency.
- 102. The system described and in use by the Government infringes one or more of the '980 Patent claims, including, by way of example, and not limitation, Claim 31, because the system includes a method of securing a location comprising the steps of:
 - a. generating real-time imagery of a secured location;
 - b. transmitting the real-time imagery to a security system central monitoring station over a network connection;
 - c. processing the real-time imagery at the security system central station;
 - d. transmitting the real-time imagery from the security system central station to a response agency over a network connection; and
- 103. displaying the real-time imagery at the response agency, wherein the response agency is identified from amongst a plurality of response agencies by a computer system at the security system central station.

GOVERNMENT CONTRACTS WITH THIRD PARTIES

104. The Government contracts with outside vendors to obtain hardware components, software and other components needed to provide security systems for secured locations.

- 105. By way of example, and not limitation, GSA Schedule 84 is for "total solutions for law enforcement, security, facilities management fire, rescue, clothing, marine craft and emergency/disaster response."
 - a. IdigoVision, a manufacturer of IP Video Surveillance Solutions, was awarded GSA approved vendor status, and GSA Contract Number GS-07F-0271Y, within the GSA Schedule 84. IndigoVision advertises that it provides a security system that includes IP video cameras, sensors, a control center to receive input from computers connected to such sensors, and the capabilities of providing real-time video of alarm events to response agencies.
 - b. Similarly, Datawatch Systems, Inc. offers many of the same services as IndigoVision and was likewise awarded GSA approved vendor status, and GSA Contract Number GS-07F-0634N, within GSA Schedule 84.
- 106. On information and belief, GSA Schedule 70 is for "general purpose commercial information technology equipment, software and services.
 - Vidsys represents on its webpage that it is received a Government contract through
 GSA Schedule 70.
 - b. On information and belief, the Government is receiving goods and services through contracts under GSA 70 and that those products and services are being used to infringe the Patents.
- 107. On information and belief, Government contracts provide specifications and terms for the services and products that are being acquired.
 - a. On information and belief, the specifications and terms of Government contracts will provide evidence of infringement.

- b. The relevant Government contracts are confidential.
- c. On information and belief, the Government contractors providing products and services for the Government's security systems are restricted from disclosing the exact nature of their activities.
- d. The Government and its contractors are operating in secrecy for the purpose of protecting government facilities and personnel.
- I. COUNT I Use or Manufacture of Inventions that infringe the '085 Patent by the United States Government through Internal Development and Deployment and/or through Development and Employment through Contractors and/or Subcontractors.
- 108. Plaintiffs reallege and incorporate by reference the allegations of Paragraphs 1-108 above, as if fully set forth herein.
- 109. Plaintiffs are the sole holders of all rights, titles, and interests in and to the '085 Patent, including all rights to enforce this patent and collect past and future damages for infringement.
- 110. The Government has been, and is now using or manufacturing the art described in and covered by the '085 Patent without license or any other lawful right.
- 111. The Government has entered into certain contracts with a number of entities who have been and are now manufacturing components or services necessary to practice the art described in and covered by the '085 Patent without license or any other right. These may include, by way of example, and not limitation, the contractors and/or subcontractors identified herein.
- 112. Plaintiffs have been, and continue to be, damaged by the Government's internal development and use of the art taught by the '085 Patent and, pursuant to 28 U.S.C. 1498, are entitled to recover reasonable and entire compensation from the United States for all infringing

inventions manufactured and used during the relevant time for which Plaintiffs are entitled to collect damages and for subsequent use.

- 113. Plaintiffs have been, and continue to be, damaged by the Government through its use of contractors and subcontractors to provide the infringing products and services necessary to practice the art taught by the '085 Patent and, pursuant to 28 U.S.C. §1498, are entitled to recover reasonable and entire compensation from the United States for all infringing inventions manufactured and used during the relevant time for which Plaintiffs are entitled to collect damages and for subsequent use.
- 114. Plaintiffs also seek reasonable litigation costs, attorney and expert witness fees, taxable costs, and delay compensation for interest computed from the time payment should have been made for the license to the '085 Patent.
 - II. COUNT II Use or Manufacture of Inventions that infringe the '344 Patent by the United States Government through Internal Development and Deployment and/or through Development and Employment through Contractors and/or Subcontractors.
- 115. Plaintiffs reallege and incorporate by reference the allegations of Paragraphs 1- 108 above, as if fully set forth herein.
- 116. Plaintiffs are the sole holders of all rights, titles, and interests in and to the '344 Patent, including all rights to enforce this patent and collect past and future damages for infringement.
- 117. The Government has been, and is now using or manufacturing the art described in and covered by the '344 Patent without license or any other lawful right.
- 118. The Government has entered into certain contracts with a number of entities who have been and are now manufacturing components or services necessary to practice the art

described in and covered by the '344 Patent without license or any other right. These may include, by way of example, and not limitation, the contractors and/or subcontractors identified herein.

- 119. Plaintiffs have been, and continue to be, damaged by the Government's internal development and use of the art taught by the '344 Patent and, pursuant to 28 U.S.C. 1498, are entitled to recover reasonable and entire compensation from the United States for all infringing inventions manufactured and used during the relevant time for which Plaintiffs are entitled to collect damages and for subsequent use.
- 120. Plaintiffs have been, and continue to be, damaged by the Government through its use of contractors and subcontractors to provide the infringing products and services necessary to practice the art taught by the '344 Patent and, pursuant to 28 U.S.C. §1498, are entitled to recover reasonable and entire compensation from the United States for all infringing inventions manufactured and used during the relevant time for which Plaintiffs are entitled to collect damages and for subsequent use.
- 121. Plaintiffs also seek reasonable litigation costs, attorney and expert witness fees, taxable costs, and delay compensation for interest computed from the time payment should have been made for the license to the '344 Patent.
 - III. COUNT III Use or Manufacture of Inventions that infringe the '980 Patent by the United States Government through Internal Development and Deployment and/or through Development and Employment through Contractors and/or Subcontractors.
- 122. Plaintiffs reallege and incorporate by reference the allegations of Paragraphs 1- 108 above, as if fully set forth herein.
- 123. Plaintiffs are the sole holders of all rights, titles, and interests in and to the '980 Patent, including all rights to enforce this patent and collect past and future damages for infringement.

- 124. The Government has been, and is now using or manufacturing the art described in and covered by the '980 Patent without license or any other lawful right.
- 125. The Government has entered into certain contracts with a number of entities who have been and are now manufacturing components or services necessary to practice the art described in and covered by the '980 Patent without license or any other right. These may include, by way of example, and not limitation, the contractors and/or subcontractors identified herein.
- 126. Plaintiffs have been, and continue to be, damaged by the Government's internal development and use of the art taught by the '980 Patent and, pursuant to 28 U.S.C. 1498, are entitled to recover reasonable and entire compensation from the United States for all infringing inventions manufactured and used during the relevant time for which Plaintiffs are entitled to collect damages and for subsequent use.
- 127. Plaintiffs have been, and continue to be, damaged by the Government through its use of contractors and subcontractors to provide the infringing products and services necessary to practice the art taught by the '980 Patent and, pursuant to 28 U.S.C. §1498, are entitled to recover reasonable and entire compensation from the United States for all infringing inventions manufactured and used during the relevant time for which Plaintiffs are entitled to collect damages and for subsequent use.
- 128. Plaintiffs also seek reasonable litigation costs, attorney and expert witness fees, taxable costs, and delay compensation for interest computed from the time payment should have been made for the license to the '980 Patent.

IV. DAMAGES

129. Based on publicly available materials on the scope of the Government's activities, and after conferring with a consulting expert on damages, Plaintiffs reasonably believe that damages approach or exceed \$1 Billion.

V. PRAYER FOR RELIEF

- 130. Plaintiffs demand the following relief:
- a. Entry of judgment that the inventions set forth in the Infringed Patents have been used and manufactured by and for the United States without license or lawful right within the meaning of 28 U.S.C. §1498;
- b. Reasonable and entire compensation for the unauthorized use and manufacture by and for the United States in an amount to be determined at trial;
- c. Plaintiffs' reasonable fees for expert witnesses and attorneys, plus its costs in accordance with 28 U.S.C. §1498 and/or the Equal Access to Justice Act, 28 U.S.C. §2412;
- d. Pre-judgment and post-judgment interest on the damages assessed; and
- e. Such other and further relief, both at law and in equity, to which Plaintiffs may be entitled.

Respectfully submitted,

/s/ Stephen A. Kennedy
Stephen A. Kennedy
KENNEDY LAW, L.L.P.
1445 Ross Avenue, Suite 2750
Dallas, TX 75202
Telephone: 214.716.4343

Fax: 214.593.2821

Counsel for Plaintiffs
3rd Eye Surveillance, LLC and
Discovery Patents, LLC

CERTIFICATE OF SERVICE

I certify that a true and correct copy of the foregoing has been served upon all counsel of record this 26th day of January via service through the ECF portal.

<u>s/ Stephen A. Kennedy</u> Stephen A. Kennedy